OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

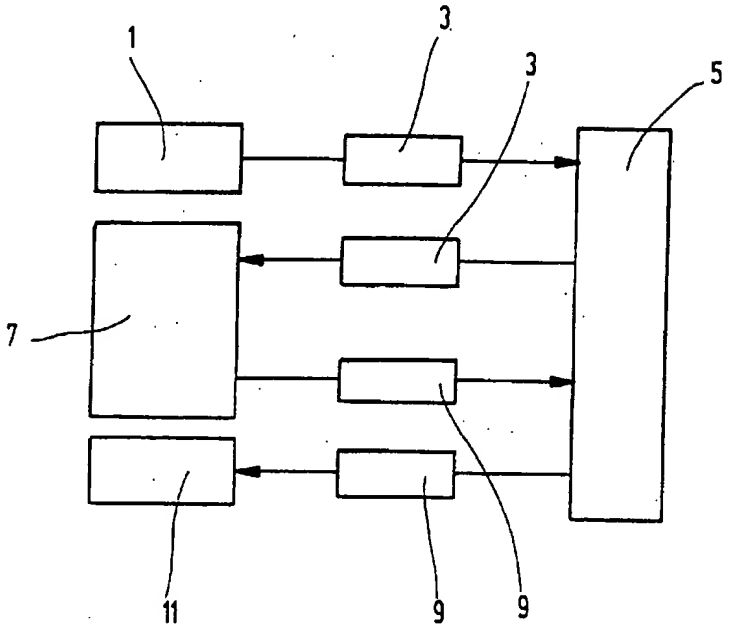
(21) (A1) **2,308,386**
(86) 1998/10/24
(87) 1999/05/06

(72) ROVER, STEFAN, DE
(72) GROFFMANN, HANS-DIETER, DE
(71) BROKAT INFOSYSTEMS AG, DE

(51) Int.Cl.[6] H04L 9/32
(30) 1997/10/28 (197 47 603.1) DE

(54) **PROCEDE POUR LA SIGNATURE NUMERIQUE D'UN MESSAGE**

(54) **METHOD FOR DIGITAL SIGNING OF A MESSAGE**



(57) L'invention concerne, un procédé pour la signature numérique d'un message, ainsi que les moyens necessaires à cet effet.

(57) The invention relates to a method and to the necessary means for digital signing of a message.

Process for Digital Signing of a Message

Description

The present invention relates to a process for the digital signing of a message and to a system required for practising this process.

Digital signatures, ie., electronic signatures, are usually made with the aid of so-called public-key processes. In these processes, to the signer there is assigned a pair of keys which consist of a secret key and a public key. A signature is generated by means of the secret key with a mathematical algorithm, and this signature can be verified with the associated public key. The secret key can be controlled only by the signer so that nobody is able to sign in the name of the signer. The public key, by contrast, may be published so that anybody can verify the signature. The secret key is usually protected through a PIN so that for making a signature, knowledge of the PIN and possession of the secret key are required.

Digital signatures can be generated in a computer, eg., in a PC, with the aid of software programs. The associated secret key is usually stored on a hard disk or a diskette and downloaded into the main memory for generating the signature. In most instances, the secret key proper is, in turn, stored in encoded form and protected via a PIN which the owner has to input when signing via the software. This is to ensure that only the owner of the secret key can use the same for signing. Since no additional hardware is required, this process is advantageous in regard to costs. It turns out to be a shortcoming that the user must rely on the signature software's integrity and that the same is not deemed sufficiently safe.

Hardware-based processes are an alternative for generating digital signatures in a computer. These processes for signing make use of special systems in which the display component and the keyboard are coupled with the signature component by hardware in a way such that the connection cannot be influenced. These systems are usually connected to the computer via a galvanic connection, eg., a cable to the serial interface. These systems have their own display component which displays the message to be signed, and their own keyboard, the so-called PIN pad through which the PIN is inputted for making the key available. The secret key is usually not stored in the signing unit but rather on a chipcard which can be introduced into the system. The signature proper can be generated on the chipcard (in the case of chipcards with incorporated cryptoprocessor) or in the system. The above-described hardware-based process forms a closed signing system consisting of the display component, the keyboard, the reader, and the chip card.

Hardware-based processes are significantly safer than software-based processes but their costs are higher. Accordingly, so-called hybrid processes are used at the present time. In these, the secret keys are in most cases stored on a chipcard and made available via a reader instrument. The other tasks, such as display, inputting of the PIN, and signature generation are fully or partially carried out in the computer. It may be provided that the signature unit, ie., the reader and the chipcard, is used as a pure storage medium for the secret key, whereas the display, the inputting of the PIN, and the generation of the signature are entirely carried out in the computer.

It can be provided as an alternative to effect the display and the inputting of the PIN through the computer; in this case, the signing unit is used for signature generation, in addition to storing the secret key. Finally, there exists a version in which only the display is effected in the computer. In this version, the signing unit has its own keyboard or it

is directly connected with the computer keyboard under exclusion of the computer software. The signature is generated in the signing unit. This process is the more cost-saving the fewer tasks must be carried out by the computer software and the lower the performance requirements to the signing unit.

WO 96/32700 discloses a process in which a message generated in a mobile radio telephone is signed digitally and passed on. EP 0 689 316 A2 discloses a process and a system for identifying and verifying data in a communication network.

However, in all this embodiments there is the basic problem that there must be signed precisely the data which the user wants to sign. It must be precluded that a virus affects the data, for example during the transmission from the display component, eg., from the display, to the signing component, eg., the cryptoprocessor. Furthermore, it must be ensured that a secret number (eg., the PIN), which is required to trigger signatures, cannot be read from the keyboard by other programs and does not become known to third parties.

Furthermore, the large-scale utilisation of the option of digital signing is limited by the comparatively small distribution of signing units. In fields of the potential application of digital signatures, eg., in internet banking, therefore a costly infrastructure would have to be set up to spread the use of signing units. Also the installation of signing units at the computer is problematic. On the one hand, the units must be physically connected to the computer, yet all the serial interfaces of a PC are often already in use. Alternative processes for incorporating signing units in computers are likewise problematic, since for this purpose software drivers and, sometimes, even additional hardware are required. Apart from this, for all signing units there must be implemented special software components which allow the application program to communicate with the signing unit.

A further problem of the conventional processes for digital signatures results from the fact that they are location-dependent. Particular fields of application of digital signatures, eg., internet banking, are location-independent in view of the everywhere accessible public internet terminals. If these internet banking applications were combined with the known location-dependent processes for digital signing, independence of the location would be lost in these applications.

A low cost, easy-to-build, and location-independent process for the digital signing of communications and the provision of appropriate means are the technological problems underlying the present invention.

These technological problems are solved through the teachings according to the main claim. Thus, the invention creates a process for digital signing of a message by means of a signing unit, which message is to be transmitted to a receiver, with the message to be signed being transmitted from a transmitter to a receiver, this message thereafter being transmitted from the receiver via a telephone network, particularly the mobile radio telephone network, to a signing unit associated with the transmitter, this message then being signed in the signing unit and retransmitted, as signed message, to the receiver. In a particularly preferred embodiment of the invention, the signing unit is a mobile radio telephone and, accordingly, the mobile radio phone network is the telephone network.

In the context of the present invention, digital signing of a message is understood as a procedure in which the intent to deliver a message and its contents are confirmed electronically. This is effected by partial or full encoding of the message to be signed or by encoding of a cryptographic check sum of this message into a signed message by means of a secret key and by making use of an algorithm. In the context of the present invention, a signed message is understood either as the message as a whole or as the signature proper. Signing serves for being able to identify the user later on. In the context of the present invention, a signed message is understood also as merely the electronically generated signature of the message. In the context of the present invention, a message is understood as any kind of electronically reproducible information, for example, numbers, characters, combinations of numbers, combinations of characters, graphs, tables, etc. In the context of the present invention, a signing unit is understood as a unit which

can perform the signing of the message, ie., which comprises a secret key, a mathematical encoding procedure, facilities for dialog with the signer or user, optionally the required interfaces, and a transmitting and receiving system. This unit can be composed of various elements, for example, of a chipcard and a reader or a chipcard and a mobile radio telephone. In the context of the present invention, signing means are understood as a component of the signing unit, including the secret key and/or the encoding procedure and/or an interface with the two or one of the aforementioned components

Based on the - according to the invention particularly preferred - use of the radio telephone net for transmitting messages to be signed to a signing unit, which, in an advantageous embodiment is a mobile radio telephone, it is possible to transmit messages to the signing unit from a commercial computer having a connection to an appropriate message server, eg., by e-mail, without need for implementing or modifying anything at the computer.

In a particularly preferred embodiment, the invention envisages a process of the above-identified type in which the message to be signed is transmitted, from a transmitter to be termed a message source, eg , a PC, to a receiver, eg., a message server, in which this message is thereafter transmitted from the receiver to a signing unit associated with the transmitter, particularly to a mobile radio telephone, with this message thereafter signed in the mobile radio telephone and retransmitted to the receiver as signature, ie., as signed message.

Thus, the invention provides that an unsigned message or a message to be signed is transmitted from a message source to a receiver, for example, to a message server. Then the receiver associates the message to be signed with the signing unit, particularly with the mobile radio telephone. This is effected either via documentation stored in the receiver or via information which, together with the message to be signed, was transmitted from the transmitter to the receiver. The association of the signing unit, advantageously of the mobile radio telephone, with the message source therefore need not be a spacewise localised association but is an association purely through information. The association involves the determination of the signing unit and, hence, of the user who has to sign the received message to be signed. The mobile radio telephone which is used in the preferred embodiment of the invention can advantageously display a message to be signed and, when instructed by the user, can effect the signing with the aid of the advantageously employed chipcard. The message signed in this way is transmitted to the receiver and there optionally compared with the original message and identified as authentic. The signed message, which is optionally identified as authentic, is then transferred to an addressee.

The invention also relates to an above indicated process in which it is provided in advantageous fashion to use a public-key process for signing, wherein the transmitter has an associated secret key and the receiver has a corresponding public key associated with the secret key. This procedure has the advantage of not necessitating the transmission of the keys.

In a further advantageous embodiment, the invention relates to an above-indicated process in which the message to be signed, or the previously signed message, ie., for example, the signature, is transmitted between the receiver and the signing unit, particularly the mobile radio telephone, by means of short-message service (SMS). In a particularly preferred embodiment, it can be provided

that both the transmission of the message to be signed from the receiver to the mobile radio telephone and the transmission of the signed message or of the signature from the mobile radio telephone to the receiver are carried out by SMS.

In a further embodiment, the invention provides that the message to be signed is displayed by means of a display provided in the mobile radio telephone. This can be the display of conventional mobile radio telephones. In this way, simple texts, such as, for example, banking transactions or even simple graphs, can be readily displayed.

Following this optionally provided display, the user gives an appropriate instruction in a corresponding dialog for triggering the signing operation. In a particularly preferred embodiment, the invention provides a process of the above-indicated type in which the secret key required for signing is stored in a chipcard of the mobile radio telephone and in which this key is activated by means of a secret number (termed PIN in what follows) capable of being inputted from the key pad of the mobile radio telephone. By corresponding appropriate programming of the mobile radio telephone it can be ensured in advantageous fashion that the inputted PIN is transmitted only to the chipcard and cannot be recognised from the outside.

In a further alternative embodiment of the aforementioned process according to the invention, it is provided to input the secret key required for signing via the key pad of the mobile radio telephone.

It is provided in a further preferred embodiment of the invention that in one of the aforementioned processes, the secret key is stored not only on the chipcard of the mobile radio telephone but that there also the signing of the message is effected. In this way it is ensured in advantageous fashion that the secret key does in no event leave the chipcard and therefore cannot be used by unauthorised persons.

It is provided in a further preferred embodiment of the invention that the mobile radio telephone is used not only for signing the message but, in addition, as the sender for transmitting the signed message to the receiver.

The invention also relates to means for practising the aforementioned processes, particularly mobile radio telephones and chipcards.

In a further preferred embodiment of the invention there is provided a mobile radio telephone which comprises a key pad, display means, and chipcard means for reading and/or writing of a chipcard adapted to be inserted into the mobile radio telephone, wherein there are provided, in addition, signing means which are suitable, for example, for communicating with a chipcard according to the invention and/or for generating a signed message from a message to be signed. The signing means are advantageously connected with the key pad for inputting a secret key or a PIN.

In a particularly advantageous embodiment of the aforementioned mobile radio telephone, it is provided that the signing means represent a software component at variance with the conventional software component of a mobile radio telephone. In a preferred embodiment of the invention, this modified software component is suitable for carrying out the signing of the message after dialog with the user. In a further embodiment, the modified software component, which is provided according to the invention, is advantageously capable of communicating with the chipcard according to the invention for carrying out the signing according to the invention. It is provided in a particularly

advantageous embodiment of the invention that the signing means of the signing unit can work with additional algorithms which facilitate the display of the message to be signed on the display field of the mobile radio telephone.

Thus, the present invention in particularly advantageous fashion makes available a system in which only the software components have to be modified relative to the conventionally employed software components. No modification of the hardware is required.

In a further embodiment of the invention, the invention also relates to the chipcard for mobile radio telephones, particularly for the aforementioned mobile radio telephones, wherein the chipcard comprises signing means capable of storing the secret key of the user. Advantageously, the signing means of the chip card are additionally capable of generating a signed message from a message received by the mobile radio telephone, ie., from a message to be signed. In the context of the present invention, the signing means of a chipcard according to the invention are understood as means which store the secret key of the user and, in an advantageous embodiment, also carry out the signing. The signing need not be carried out directly on the chip card but can be effected by a software component and/or hardware component in the mobile radio telephone.

Other advantageous embodiments of the invention will become obvious from the dependent claims.

The invention will be explained in detail with reference to the figures and the associated exemplary embodiment.

The figures show:

Figure 1, the operational sequence of the process according to the invention;

Figure 2, the schematic structure of a mobile radio telephone according to the invention; and

Figure 3, a schematic representation of a chip card according to the invention.

Figure 1 shows the transmitter 1 which can be configured as a PC having a text editor or a home banking program, a message 2 to be signed, a receiver 3 which is configured as a message server, a mobile radio telephone 7, a signed message 9, and an addressee 11.

A message 3 to be signed is sent, eg., by e-mail, to the receiver 3 with the aid of the homebanking program incorporated in the transmitter 1. The receiver 5 converts the received message, which is to be signed, into a message which can be sent to the mobile radio telephone 7, particularly by means of a mobile-phone radio net, and though SMS, in an advantageous embodiment. The receiver 5 associates the message 3 to be signed with the mobile radio telephone 7, for example by means of data stored in the receiver 5. It may also be provided that the association is effected by means of data sent by the transmitter 1 together with the message to be signed. These data are, in general, the phone number of the mobile radio telephone.

The received message 3 is displayed in the mobile radio telephone 7 on a display 13. The precise operation will be explained in detail in the description pertaining to Figure 2. After displaying the message 3 to be signed on the display 13, the message 3 to be signed is being signed upon instruction by the user and the signed message 9 is passed on to the receiver 5 or to some other receiver. Transmission of the signed message 9 from the mobile radio telephone 7 to the receiver 5 is likewise effected though SMS. The receiver 5 is capable of comparing the signed message 9 with the

original message 3 to be signed and transmit it thereafter to an addressee 11. Transmission to the addressee 11 can be carried out in any form.

Figure 2 illustrates a mobile radio telephone 7. The mobile radio telephone 7 comprises a display 13, a transmitter/receiver 15, chipcard means 17, a key pad 19, and signing means 21.

The message 3 to be signed, which is transmitted from the receiver 5, is received by the transmitter/receiver 15 of the mobile radio telephone 7 and, if necessary, passed on in modified form to the signing means 21. The signing means 21 take care of the internal control of the signing operation. The signing means 21 comprise software components for controlling the display 13 so that the message 3 to be signed can be made visible. Furthermore, the message 3 to be signed is signed within the signing means 21. In order to be able to carry out the signing operation, the signing means 21 must communicate with the chipcard means 17. Furthermore, it is necessary that the secret key proper or the PIN is inputted to the signing means 21 via the key pad. If the PIN, which is usually shorter, ie., which has fewer digits than the secret key, is inputted by the user via the key pad 19, the PIN can - so to speak - activate the unwieldy secret key for the signing operation by means of the operating system of the chipcard 25. The signing means 21 can communicate with the chipcard 25 via a bidirectional connection line 23. The chipcard means 27 ensure that the commands of the signing means 21 are executed and that the signed message 9 is passed on to the transmitter/receiver 15 via the signing means 21. This means that the chipcard means 27 form an interface between the signing means 21 and the chipcard 25.

Figure 3 shows - in very simplified, schematic form - a chipcard 25 according to the invention. It comprises basically a contact pad 31, a memory unit 27, and a cryptography module 29. The secret key required for generating the signed message 9 is stored in the memory unit 27. The cryptography module 29 serves for encoding the message 3 to be signed, for example, by means of an RSA process. The memory unit 27 or the cryptography module 29 can communicate with the chipcard 27 via the contact pad 31. Other elements required for the operation of the chipcard 25, eg., a controller, are not shown in Figure 3 for the sake of clarity of the representation.

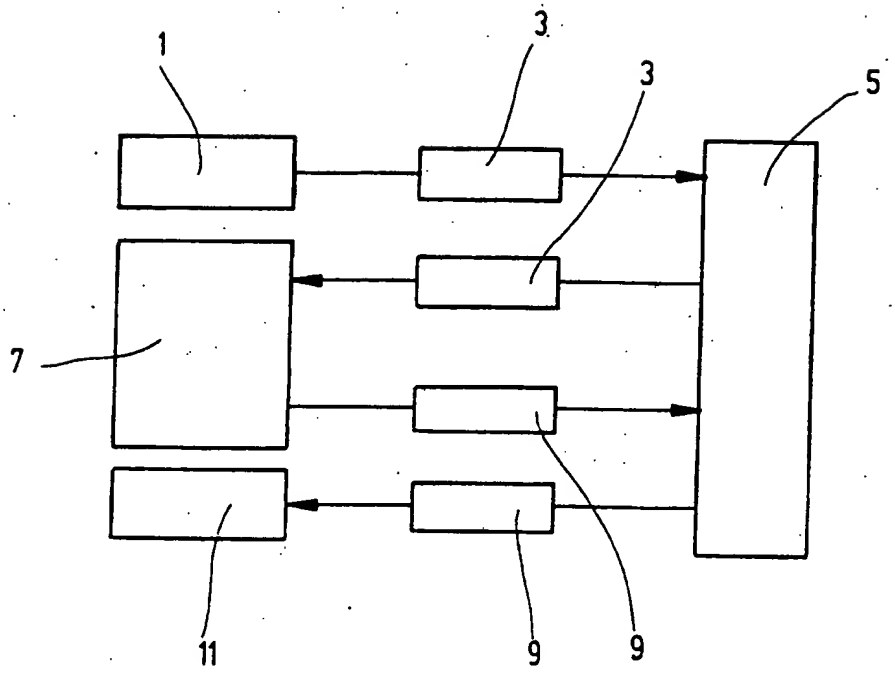


Fig. 1

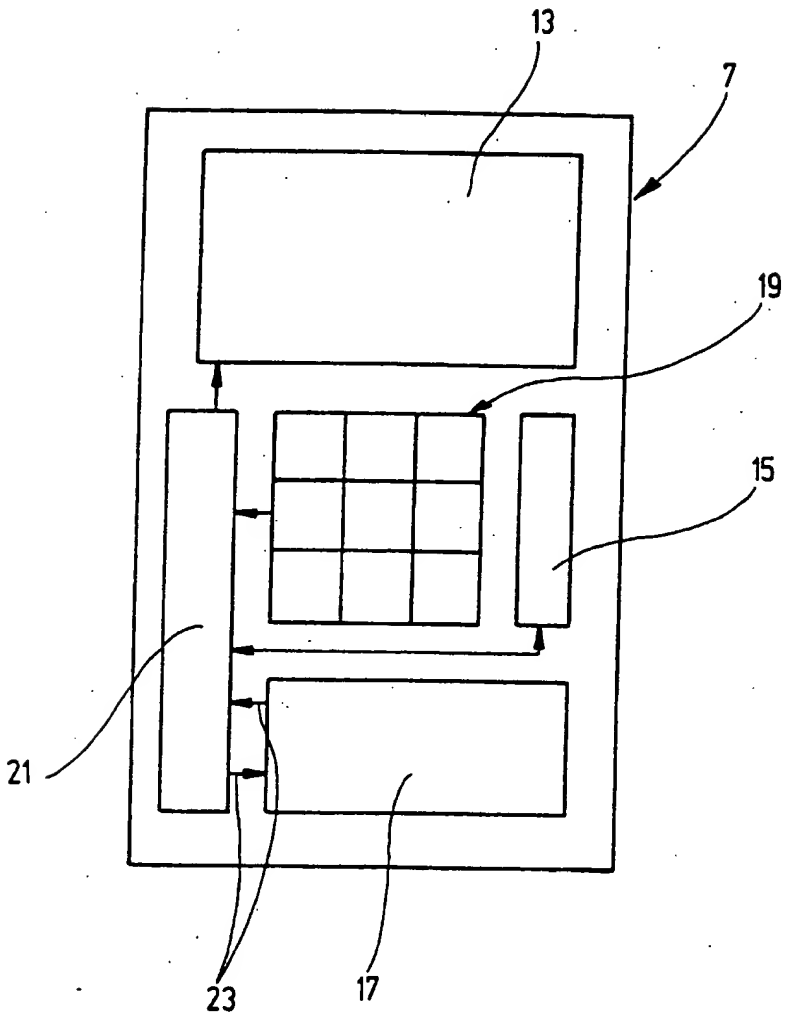


Fig. 2

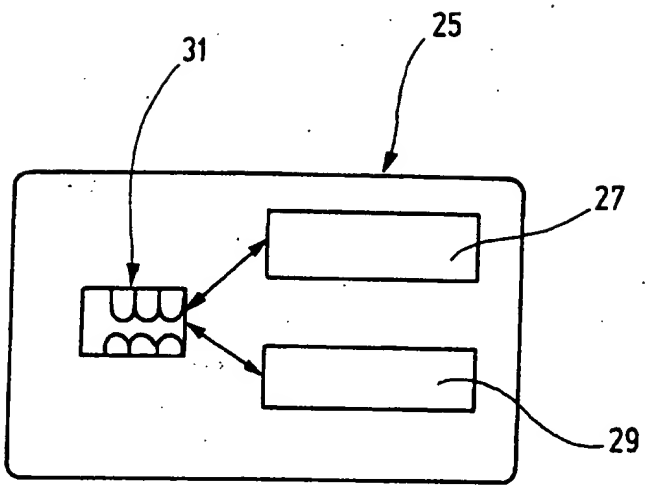


Fig. 3

Claims

1. A process for the digital signing of a message by means of a signing unit, with the message to be transmitted to a receiver, characterised in that the message (3) to be signed is transmitted from a transmitter (1) to a receiver (5), this message is thereafter transmitted from the receiver (5) via a telephone network to a signing unit associated with the transmitter (1), this message is then signed in the signing unit and retransmitted, as signed message (9), to the receiver (5).

2. The process according to claim 1, wherein the signing unit is a mobile radio telephone (7).

3. The process according to claim 2, wherein the telephone network is a mobile radio telephone network.

4. The process according to any one of the preceding claims, wherein a public-key process is used for signing, particularly a public-key process in which the transmitter (1) has an associated secret key and the receiver (5) has a corresponding public key matching the secret key.

5. The process according to any one of the preceding claims, wherein the messages are transmitted between the receiver (5) and the mobile radio telephone (7) by means of the short-message service (SMS).

6. The process according to any one of the preceding claims, wherein, prior to signing, the message (3) is displayed by means of a display (13) provided in the mobile radio telephone (7).

7. The process according to any one of the preceding claims, wherein the secret key required for signing is inputted via keyboard means of the mobile radio telephone (7).

8. The process according to any one of the preceding claims, wherein the secret key required for signing is stored on a chipcard of the mobile radio telephone (7) and this key is activated by means of a PIN adapted to be inputted via keyboard means of the mobile radio telephone (7).

9. The process according to any one of the preceding claims, wherein the chipcard carries out the generation of the signed message (9).

10. The process according to any one of the preceding claims, wherein the mobile radio telephone (7) generates the signed message (9) and wherein the secret key is read from the chipcard (25).

11. The process according to any one of the preceding claims, wherein the mobile radio telephone (7) serves, in addition, as the sender for transmitting the signed message (9) to the receiver (5).

12. A chipcard for a mobile radio telephone, wherein the chipcard (25) comprises signing means (21) which include a memory unit (27) for storing the secret key required for generating the signed message (9), characterised in that the signing means (21) generate a signed message (9) from a message (3) which is received by the mobile radio telephone (7) via the telephone network and is to be signed.

15. The chipcard according to claim 14, characterised in that the chipcard (25) comprises signing means (21) which generate a signed message (9) from a message which is received by the mobile radio telephone and is to be signed.

ABSTRACT OF THE DISCLOSURE

The invention relates to a method and to the necessary means for digital signing of a message.